2-18-00 A

SKJERVEN
MORRILL
MACPHERSON
FRANKLIN
& FRIEL LLP

Docket No.: M-7348 US

February 16, 2000

Box Patent Application
Assistant Commissioner for Patents
Washington, D. C. 20231

Enclosed herewith for filing is a patent application, as follows:

Inventor(s): Mark Alan Hollar and Peter Wonfor

Title: Method And Apparatus For Enhanced Audio/Video Services With Watermarks And Associated Data

X	Return Receipt Postcard
X	This Transmittal Letter (in duplicate)
18	page(s) Specification (not including claims)
9	page(s) Claims
1	page Abstract
3	page(s) Declaration For Patent Application and Power of Attorney
9	Sheet(s) of Drawings
1	page(s) PTO Form 1449 citing one reference
X	Copy of one Cited References submitted

CLAIMS AS FILED (fees computed under §1.9(f))

For	Number Filed			Number Extra		Rate			Basic Fee
Total Claims	40	-20	=	20	x	$9.00	=	$	$345.00
								$	180.00
Independent Claims	14	-3	=	11	x	$39.00	=	$	429.00
☐ Application contains one or more multiple dependent claims (total fee)								$	

☒ Total fee for filing the patent application in the amount of $ 954.00

EXPRESS MAIL LABEL NO:
EM425671550US

Respectfully submitted,

Norman R. Klivans
Attorney for Applicants
Reg. No. 33,003

25 Metro Drive, Suite 700
San Jose, CA 95110
Phone 408 453-9200
Fax 408 453-7979

Austin, TX
Newport Beach, CA
San Francisco, CA

EXPRESS MAIL LABEL NO:
EM 425 671 550 US

METHOD AND APPARATUS FOR ENHANCED AUDIO/VIDEO SERVICES WITH WATERMARKS AND ASSOCIATED DATA

Mark Alan Hollar
Peter Wonfor

FIELD OF INVENTION

This disclosure relates to audio and video and to enhanced audio and video services, such as pay-to-record or pay-to-tape, in, e.g., a cable television system, direct broadcast satellite system, or public computer network (internet).

DESCRIPTION OF THE PRIOR ART

Some methods of controlling copying, or preventing serial copying, of video material with a video watermark rely on the recording device to add a second watermark to the video image. Watermarks are well known in the digital video field. Watermarks are signals embedded in an otherwise conventional video or audio signal that provide a unique identifier and thus discourage or prevent unauthorized copying or use. The watermark is not apparent to a person viewing the watermarked signal, but is readily detected by appropriate circuitry.

Preventing or controlling copying is useful to prevent copyright infringement, and prevent distribution of unauthorized copies. In a "generational" control system where there is a one-copy-allowed state and a no-more-copies-allowed state, the combination of first and second watermarks define the no-more-copies-allowed state while the original watermark defines the one-copy-allowed state. (Copying here refers to use of a video tape recorder or video disc recorder, for instance.) In a television system with a digital cable

television or direct broadcast satellite set top box (STB), this type of system prevents serial copying of video content, since the compliant recorder makes the appropriate state change from one-copy-allow to no-more-copies during the record process. However, it does not easily allow for a pay-to-record feature since records are generally not provided with back channel and communication mechanisms for reporting purchase choices to an accounting system.

To implement a pay-to-record feature, the STB needs to control the state change rather than the recorder controlling the state change. The pay-to-record feature thus allows a STB to output video under conditional access control with three possible payments by the viewer: No payment: the consumer (viewer) is not allowed to view or record the content; One level of payment: the consumer is allowed to view the content, but is not allowed to record it. Different (higher) payment: the consumer can both view and record the content. While it is possible to use the STB to introduce the second watermark, there are "legacy" issues that prevent widespread adoption of such a system. Specifically, there is a large installed base of STBs which do not incorporate the required features to allow this second watermark to be added. If a copy control system were introduced which used such a second watermark for copy control in STBs, then the existing consumers with STBs without this feature would be disenfranchised; those consumers would be unable to make copies at all.

An alternative method of providing these copy control features uses a "ticket." A ticket here is a cryptographic counter (number, usually in binary form) which is carried in a communications channel associated with the video. This ticket uses one-way cryptographic

features to maintain a play and record history. One way functions are well known to those versed in the cryptographic field and include a class of transforms with the property that the function is relatively easy to compute but significantly harder to undo or reverse. In other words, given x it is easy to calculate f(x), however given f(x) it is difficult to compute x.

A recorder detecting the one-copy-allowed state's watermark must then detect the correct ticket prior to allowing a recording to be made. To convey the ticket from the STB to the recorder, the vertical blanking interval (VBI) of the video signal can be used as a communications channel. However, this has the disadvantage that some broadcast MPEG encoders (video compression devices) do not transmit the entire VBI. Alternatively, the ticket is inserted in the active picture area, such that it is in the overscan area of older TV's. However, this has the disadvantage that this data may be seen by the viewer on newer TV's (having less overscan) and thus may be deemed objectionable by the consumer.

Yet another method of conveying the ticket is to activate and de-activate a subset of the analog anti-copying protection system signals to convey a bitstream. (Analog anti-copying protection signals here refer, e.g., to the Macrovision Corp. video copy protection processes which are commercially available; also see, e.g., Ryan U.S. Patent 4,601,603). This has the advantage that existing digital recorders such as those of the DVCAM type automatically delete this form of a ticket, since they fail to record the VBI. However, to accomplish the appropriate control out of the STB requires changes to the STB's internal software. In some cases, this software can be downloaded to existing

STBs over the air or cable. In this manner the encoder IC (integrated circuit) which generates the Macrovision Corp. analog copy protection pulses can react appropriately. However, in other cases the internal software has been installed permanently in the STB and cannot be modified.

All these methods of transmitting a ticket require modification to the cable-TV/satellite system head end control software to provide a way to introduce the ticket into the video. This modification could undesirably be quite expensive to the cable-TV or satellite system operator.

SUMMARY

This disclosure is directed to use of a watermark together with consumer controllable information in a television (or audio only) STB to provide pay-to-tape (or pay-to-record generally) control. One embodiment uses the existing video line 21 (in NTSC-TV) extended data service or closed caption protocol to hold a ticket (cryptographic value), and a video watermark, to jointly control copying of video being provided by a STB. This may be done in such a manner to enable additional features, such as pay-to-tape or pay-to-record, even in systems with prior art (legacy) STBs. In addition, this approach has the advantage that existing cable-TV or satellite system head end MPEG (compression) encoders can already transmit this type of information. Hence minimum changes are required to the system operator's infrastructure.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1A shows a block diagram of a system in accordance with the disclosure; Figure 1B shows detail

of Figure 1A; Figure 1C shows a variant of Figure 1A; Figure 1D shows a variant of Figure 1C.

Figure 2 shows playback in accordance with this disclosure.

Figure 3 shows a video recorder for the Figure 1A system.

Figure 4 shows a block diagram of another system.

Figure 5 shows a video recorder for the Figure 4 system.

Figure 6A shows the system of Figure 1; Figure 6B shows a combination STB and recorder.

Figure 7 shows the system of Figure 4 modified for audio.

Figure 8 shows an audio recorder for the Figure 7 system.

DETAILED DESCRIPTION

This disclosure is of a system which in one embodiment utilizes the existing infrastructure and legal advantage given to video line 21 (in the VBI in NTSC-TV) data and combines it with a new aspect available with video watermarks to generate revenue by allowing controlled copying of video signals. Video line 21 (in NTSC TV, which is the U.S. television standard) currently is used to carry closed caption data and parental blocking (V-chip) data in accordance with two significant standards: ANSI/EIA-608 and ANSI/EIA-744. (Other television standards have similar features and may be used similarly.) In particular, various U.S. laws require television sets sold in the U.S. to react to data carried by line 21 and require the data on line 21 to be preserved during transmission through various paths. In addition, U.S. FCC rules derived from the U.S. Telecommunications Act of 1996 also require TV

receivers or PC's (personal computers) with video tuner cards, and with displays greater then 13" in size, to provide parental blocking (V-Chip control).

The legal requirement (in the U.S., at least) to provide parental blocking ensures that PC's (personal computers), as a potential class of storage/recording device, must recognize video line 21 data. Without this legal requirement, PC's might make that bandwidth/capacity available for other functions. As described in EIA-608, field 1, line 21 is allowed only to have closed captioning or the original picture content. (TV pictures have two fields per frame.) No other data services are allowed here. Field 2, line 21 may however have closed captioning, parental blocking or other extended data services. The protocol provided with extended data services is flexible enough that the protocol can accommodate a ticket (or other associated data) as described above.

To follow the path of the ticket as shown in Figure 1A, at the time of content (program) preparation by the content provider 10, a seed (number) S is generated by a seed generator 12. (This is, e.g., a random number generator.) This seed S is then subject to a fixed and secure one-way hash function F by hash function element 16. This is a one-way hash (compression) function of the type well known in the cryptographic field to determine the original ticket T. The system operator cannot reliably be known to be a trusted party; as such, making the seed accessible to him has the potential to weaken the system security. Hence in this embodiment the content provider, not the system operator, does this. In addition, the seed S is provided to the watermark embedder 20.

Note that this is a hybrid digital-analog TV system. Upstream of the STB 34, the signal is digital; the STB outputs an analog signal or optionally both a digital and analog form of the video signal. Signal transmission over other channels (e.g., the internet) is an alternative.

Each block in the figures represents a conventional integrated circuit or commercially available component (circuit or software) or product or such a conventional element modified as disclosed here; the nature of the connections therebetween as shown in the figures, and any necessary modification thereto, will be apparent to one skilled in the art in light of this disclosure. For instance, the content provider block 10 could be embodied in a suitably modified computer, with the seed, ticket and watermark generation carried out by software executed by the computer's central processing unit.

The watermark embedder 20 submits the seed S recursively to the function F three times, as shown in detail in Figure 1B, to generate a watermark W which is then conventionally added to (embedded in) the video signal V applied at video input port 24. As shown in Figure 1B, watermark embedder 20 includes the three one way hash function F blocks 22a, 22b, 22c and element 23, which inserts the resulting data F[F(F(S))] as the watermark in the video. The output signal of embedder 23 is on line 27, also shown in Figure 1A. The watermark is added in a linear or non-linear fashion using any available watermarking technique. In some cases, to convey a sufficient number of bits to guarantee a ticket of appropriate cryptographic complexity, the ticket is transmitted as a series of characters varying over time. These digital communication methods for conveying m-bytes of data

across an n-bit wide interface are well understood, and can use any available protocol, including, for instance, TCP/IP or PPP.

The video signal with the watermark V+W and the ticket T can be independently transmitted to the system (cable or satellite TV) operator/head end 30, or optionally the content provider can use a standard closed captioning encoder to embed the ticket T on, e.g., video line 21. (The distinction here between the content provider and system operator is arbitrary and only for purposes of illustration.) An example of a method of independent transmitting the ticket T to the system operator would be to provide it on a floppy disk. The system operator could then send it through the system as MPEG user data.

The line 21 method of distributing the ticket, as seen in Figure 1C, has the advantage that it allows the system operator to deploy the watermark/ticket addition system at its head end 30 with no changes to the remainder of its existing infrastructure. (Figure 1C is otherwise identical to Figure 1A.) In this second case, the (ticket T) data on line 21 of the video is extracted from the video signal and sent as MPEG data by the system's MPEG encoder. Without this, line 21 would be treated like video and would potentially be subject to the usual video compression artifacts, as transforms like the discrete cosine transform are applied, quantizations are made and bit rate reduction occurs. This undesirably would corrupt the ticket.

In Figure 1C, from the system operator's head end 30, the ticket T is conveyed as line 21 MPEG data in the MPEG stream's video elementary stream while the video with watermark V+W is sent as compressed picture data.

The ticket T is provided to all STBs 34 via conventional broadcast and reception of the MPEG data stream.

Two classes of STBs 34 must be considered: legacy (old) STBs and new (upgraded) STBs. Legacy STBs are unable to have their internal microcontroller software upgraded. Thus they treat the ticket T on line 21 as standard closed caption, teletext or extended data. All of this information which is provided to the STB is output in the analog video signal as line 21 data.

Consumers with legacy STBs are not inconvenienced or prevented from making a recording. This is a disadvantage from the content provider's standpoint, since he may in fact accrue less revenue as a result. However, television industry practice with respect to time shifting (video recording) may indicate that such consumers should not be disadvantaged. Thus the system as described here ensures that the consumer is in fact not disadvantaged and that legacy STBs provide the ticket on their video output. As shown in Figures 1A, 1C and 1D, the STB 34 outputs the video with the watermark with the ticket, V+W+T. In the case of Figure 1D, the ticket T is not controllable by the consumer due to the "legacy" design of the STB 34a. Here the only possible user control is pay-and-view or not-pay-and-not-view. This is controlled by the switch 41 shown in the STB 34a of Figure 1D.

New or upgraded STBs in accordance with this disclosure provide additional control to the consumer and also allow accrual of greater revenue for the system operator and lot content provider. In this case, the consumer can select whether he wishes to simply view the program or whether he wishes to view and record/store it. When he makes his selection through a standard interface with an onscreen display and remote control,

the STBs conditional access (CA) sub-system 36 stores an indicator of the activity - view only or view and record - which the consumer selected.

This indicator is transmitted to the system operator via a conventional cable/satellite TV/internet return path 39 (Figures 1A, 1C) which includes, e.g., a telephone modem using the telephone lines or, in those cable TV systems which support it, a conventional cable plant return path. Return path 39 allows the system operator to charge the consumer for his selection. A report of the access is made to the conventional system operator accounting system 35 for consumer billing purposes, via return path 39.

After the conditional access sub-system 36 has stored the indication of the consumer's request, then the addition of the ticket T to the video occurs. If the content is only to be viewed, then the video is provided out of the STB 34 without the ticket: V+W. If the content is to be viewed and recorded, then the video is provided out of the STB 34 with the ticket: V+W+T. Adding the ticket T to the video V consists now of either introducing the ticket data T in the encoder IC (integrated circuit) in the STB 34 or alternatively in an ATSC RF remodulator integrated circuit located in STB 34. It is this encoder IC which outputs an analog video signal to the associated TV receiver (not shown) connected to STB 34 based on the input digital video signal. It is the RF remodulator which outputs an ATSC digital TV signal. In this case, the ticket T is controllable by the consumer via his STB 34.

In Figures 1A and 1C the recorder 42 now receives the analog video signal V+W or V+W+T. Video recorder 42 (portions of which are shown in detail in Figure 3) is mostly conventional but adapted as disclosed here to

include the record control function 43. Ticket/line 21 data extractor 48 extracts the ticket T and submits it to circuitry (processor) 54, 56 which performs the one-way hash function F two times on ticket T. If the result of this hashing at 54, 56 matches, at comparator 57, the watermark W in the video signal detected by a watermark detector 50, then switch 58 is closed and recording by recorder 42 is allowed, i.e., recording is allowed when the following conditional logic statement is returned as being true:

$$W=F(F[T])$$

As shown, switch 58 (when closed), controlled by comparator 57, couples the V+W signal extracted by the ticket/line 21 detector circuitry 52 to the output terminal of switch 58. This output signal V+W is then coupled to the actual recording part (not shown) of recorder 42, which is conventional.

The pay-to-record feature has now been implemented. If there is no ticket T detected by the record control 43 recorder 42, then this statement (comparison) is returned as no. This would be the case if the consumer had chosen to only view the content. If the wrong ticket T is accompanying the video, perhaps because a recording of the video signal has already been made, then again the statement is returned as false and the recording is not permitted. (Note that recorder 42 need not be a digital recorder.) When recording the video and ticket to the recorder media 46 (in this case the media is a disc as shown in Figure 1A), the ticket T is again subject to the function F to generate a new version of the ticket T'. In this case the cryptographic counter has been incremented: $T' = F(T)$.

Later when playing back the video content from the recording media 46 as shown in Figure 2, circuitry associated with the drive 50 in the player 52 (e.g., a DVD player) again increments the ticket T by applying function F to it: $T'' = F(T')$. The drive 50 performs this function, e.g., when a DVD player 52 is implemented as a drive in a personal computer with a software or hardware associated MPEG decoder. (Note that there is no requirement for a drive and rotating media; the media may be, e.g., semiconductor storage with appropriate access circuit circuitry.) In any case, there is conventionally an interface (the drive or semiconductor storage control circuitry) to the actual recording (storage) medium.

Then the drive (or appropriate circuitry) performs the ticket incrementing to enhance security. (The player 52 may be the recorder 42 of Figure 1A or a play only device.) Now at the MPEG decoder 54 in the player 52, the watermark W is again detected and checked against the current ticket T''. If a match is found, then playing is allowed and play control is implemented. In this case, the following equation must hold:

$$W = T'' = F(T') = F (F(T))$$

An additional option under play control (also shown in Figure 2) at this point is to apply to the video signal an analog video copy protection of the type available from Macrovision Corporation, such as automatic gain control and/or color stripe. This has the advantage that further VHS analog video copies are prevented (or at least are not usable) as well as the additional digital copies which are worked upon by equipment with watermark detectors.

The watermark described herein can be implemented in a number of different ways, depending on the capability of the associated watermarking system. For instance, if the watermarking system that is available is able to carry sufficient data on a single field, then a sufficiently large amount of data can be carried such that no time varying mechanisms need be applied. In some embodiments the watermarking system carries 8-bits per frame; however only 4 bits are available for hashing seed purposes since 4 bits were needed for other uses. For security reasons it is desirable to use a 64-bit seed and 64-bit tickets. Thus, these embodiments require a minimum of 16 frames with the actual number of frames dependent on the transport protocol employed based on the digital communication system design. Thus one embodiment requires typical communication protocols such as PPP which employ start and stop characteristics. Due to the nature of a video communication channel, it may be desirable to employ some form of forward error correction. Reed-Solomon encoding is one example of a forward error correction code that is commonly used for this purpose.

Some embodiments also employ 16-bits per field when carrying the ticket on line 21. Thus, both the ticket processing and watermark processing require buffers for storage such that decisions can be delayed and timed to occur when whole data values are available. Design of these types of buffers is apparent to those in the video and digital communications fields in light of this disclosure.

While the above disclosure is of a method using line 21 of analog video to carry the ticket between the STB and recorder to enable pay-to-record features, any combination of a watermark and consumer controllable

information in an STB could be used. This approach is also not limited to any particular TV standard. In particular, other video lines could be used to hold the ticket as long as they have the desired characteristics of being transmitted to the STB in a manner such that they can be controlled by the consumer through the STB.

In addition, if the video is being transmitted over a digital interface, such as IEEE-1394 ("Firewire") or an ATSC (high definition TV) 8-VSB signal, from the STB to a device (recorder) which has storage capability then the ticket can still be controlled in the STB. In this case, the transmission or lack of transmission of the correct ticket is accomplished and the watermark/ticket combination still defines the copy-state. In these situations, the ticket could be transmitted using the MPEG User_data descriptor. In some cases, it may be desirable to not transmit any ticket at all, but in other cases, it may be desirable to transmit an incorrect ticket.

There are also other places in these video signals which could be used to transmit the ticket; however, the ticket is still controlled in the STB. The STB provides a way for ensuring that the content owner receives payment, whether that payment is for viewing only or for viewing and recording. Thus, it is the watermark and associated data under consumer control in the STB which are used in this method.

Another embodiment (see Figure 4) uses a second watermark embedder located in the STB 34 as a watermark remarker 60. (No ticket is used here.) In this method of creating video and record or view only video, a second watermark W2 is used. (Figure 4 shows elements identical to those used in Figure 1A, or similar, and

thereby having reference numbers similar to those of Figure 1A with the letter "a" appended.)

In the Figure 4 system, when the consumer selection 61 is to view (but not record), the analog video signal output from the STB 34a is No-More-Copy: V+W1+W2. When the consumer selection 61 is to view and record, the video signal output from the STB 34a is Copy-Once: V+W1. Under these circumstances, the record control portion 64 of the associated recorder 42a operates as shown in detail in Figure 5. (The remainder of recorder 429 is conventional.)

A watermark W1 detector 66 first detects watermark W1. If no watermark W1 is found, then recording (copying) is allowed since it is assumed free-copying is available or the content has no copyright restrictions. If watermark W1 is detected at 68, then the watermark W2 detector 72 detects watermark W2. If W2 is not detected, then recording is allowed since this defines the one-copy-allowed state. The system "fails safe" in that recording is allowed. Note that W is typically some predetermined function of the active video. The fail safe provision is so that the user is not unnecessarily inconvenienced by false positive watermark detections. In general, watermarks are "woven into the fabric" of the video image. Removing them without degrading the base active video content is very difficult.

If W2 is detected along with W1 at 72, then no recording is allowed since this defines the no-more copies state. This is accomplished by controlling switch 76, which in this case (yes from comparator 70) is set to be open. Otherwise (recording permitted) switch 76 is closed and video signal V+W1+W2 from W2 embedder 74 is output from switch 76 to be recorded by

the remaining (not shown) conventional portions of recorder 42a. If the video signal input to the recorder 42a has W1 but no W2 and is recorded on the media 46a, then the watermark W2 is embedded in the video signal prior to recording on the media 46a.

Also, it should be recognized that in Figure 5, while separate detectors 66, 72 are shown for W1 and W2, these may in fact be implemented in the same functional hardware (or software) element with internal reconfiguration as to allow differentiation of W1 and W2. This implementation is readily achieved by one skilled in the art. Playback of media using this embodiment is simpler but it provides a lower level of security since no checking or detection of the watermarks is required. Also, in many cases a compliant recorder will be coupled to the player and will thereby prevent subsequent copies from being generated. A system without this coupling still has value since record control can still provide value even without the added value of play control.

While the above described systems are disclosed in the context of separate devices for the set top box (STB) and the recorder, there is nothing to preclude the functionality of both these devices being integrated into a single apparatus. Figure 6A shows the system as described above using the same reference numbers, but also showing the compliant player 80, which outputs as shown when playing the media 46, the video with the watermark and the ticket (V+W+T").

Figure 6B shows a related system having the STB 34 combined with the recorder 42 in a single apparatus 84. As shown, the output signal stream from the recorder/player 42 may be applied to a recorder 88 if W=F(F(T)). Similarly, the media 46 may be played on

player 86 outputting the video stream as shown, which is the video with the watermark and ticket (V+W+T") or merely the video with the watermark (V+W).

It is apparent that the systems of Figures 6A and 6B may be used in the above-described system employing the above-described first watermark and second watermark method for controlling recording.

While the above disclosure is directed to video, a similar approach using the first watermark and second watermark may be applied to controlling recording of audio. Hence Figure 7 shows a system in many respects similar to that of Figure 4, however being adapted for providing enhanced audio distribution with the possibility of paying to record. The only structure labeled identically in Figure 7 to Figure 4 is the system operator headend 30. The other structures, although somewhat similar, have been redesignated to indicate that in this case they are adapted for audio purposes.

Hence the content provider 90, which is the source of the audio material, generates copy control information CGMS which is applied to the input terminal of a watermark embedder 92, to the other terminal of which is applied ordinary audio input signal A. The resulting output audio with watermark A+W1 is communicated, via conventional channels, to the system operator headend 30. From there, the audio signal A+W1 is sent over, for instance, the satellite or cable television distribution sytem to the STB 96. STB 96 includes a conditional access system 98 to which is applied a consumer selection on line 100.

The STB 96 also includes a watermark remarker 102 which adds watermark W2 under control of conditional access system 98. The watermark remarker 102 then

outputs the watermarked audio stream in one of two forms. One form is the copy-once and the other is copy-no-more. In other words, the two forms are A+W1 or A+W1+W2, the analog audio A with or without watermark W2 but always including watermark W1. The associated compliant recorder 106 receives this analog audio signal, and under control of its record control 108, does not record if W1 and W2 are present and adds W2 to the audio if it is not present and recorder 106 is in the recording mode, thereby outputting audio stream A+W1+W2 to record on associated media 112.

Figure 8 shows a block diagram of recorder 106 with further detail, showing how the record control portion 108 of audio recorder 106 includes a watermark W1 detector 114, a watermark W2 detector 116, and a watermark W2 embedder 118. The signal output from watermark W1 detector 114 is the indication of watermark W1 being present at 122. This is logically combined at 124 with the indication of whether watermark W2 is present. Only if both watermark are present is switch 128 opened, thereby preventing recording; otherwise switch 128 is closed thereby communicating the input audio with the added watermarks A+W1+W2 on the output terminal 130 of record control portion 108. It is to be understand that Figure 8 only shows the record control portion 108 of recorder 106, the remaining portions which are not illustrated being the conventional recording portions.

This disclosure is illustrative and not limiting; further modifications will be apparent to one skilled in the art and are intended to fall within the scope of the appended claims. For instance, the present system and method are readily applied to TV and video following various standards.

CLAIMS

We claim:

1. A method of controlling copying of a video signal, comprising the acts of:

supplying the video signal;

embedding a watermark in the video signal; and

providing associated data in a predetermined location of the video signal, the associated data being related to the watermark in a predetermined manner.

2. The method of Claim 1, wherein the associated data is a cryptographic value.

3. The method of Claim 2, wherein the cryptographic value is a hash function of a seed, and the watermark is the hash function of the hash function of the hash function of the seed.

4. The method of Claim 1, wherein the predetermined location, for NTSC TV, is video line 21.

5. An apparatus for processing an input video signal to control subsequent copying thereof, comprising:

a seed generator;

a hash function generator coupled to receive a seed from the seed generator and output resulting data;

a watermark generator coupled to receive the seed and generate a watermark from the seed, and to embed the watermark in a picture portion of the input video; and

a transmission channel coupled to transmit the resulting data and the watermarked video to a receiver, the resulting data being transmitted other than in a picture portion of the video.

6. The apparatus of Claim 5, wherein the watermark is the hash function of the hash function of the hash function of the seed.

7. A method of controlling copying of a video signal having an embedded watermark and associated data, comprising the acts of:

determining if recording of the video is to be permitted; and

only if recording is permitted, transmitting the video signal and the associated data, wherein the watermark has a predetermined relationship to the associated data.

8. The method of Claim 7, wherein the associated data is a cryptographic value.

9. The method of Claim 8, wherein the cryptographic value is a hash function of a seed, and the watermark is the hash function of the hash function of the hash function of the seed.

10. The method of Claim 7, further comprising the acts of:

deciding if the recording is to be permitted;

reporting that recording is to be permitted; and

charging a fee for permitting the recording.

11. A set top box for connection to a television receiver, comprising:

an input terminal adapted to receive a video signal including a watermark and to receive associated data;

a conditional access control, having a control terminal for receiving a user selection for enabling recording of the video signal; and

a combiner having a control terminal coupled to an output terminal of the conditional access control and receiving the video signal from the input terminal, and having an output terminal, wherein the combiner outputs the video signal with or without the associated data in response to the conditional access control.

12. The set top box of Claim 11, further comprising:

a connection to an uplink, and wherein the conditional access control transmits to the uplink an indication of user selection.

13. The set top box of Claim 11, wherein the associated data is a cryptographic value.

14. The set top box of Claim 11, further comprising a video recorder coupled to record the output video signal.

15. A method of operating a video recorder, comprising the acts of:

receiving an input video signal having a watermark;

detecting the watermark;

detecting data associated with the video signal;

subjecting the data to a predetermined compression function; and

allowing recording of the input video signal only if the detected watermark matches the result of the compression function.

16. The method of Claim 15, wherein the compression function is a multiple hash function.

17. The method of Claim 15, wherein the data is on a predetermined video line in the vertical blanking interval of the video signal.

18. The method of Claim 15, wherein the data is a cryptographic value.

19. A video recorder, comprising:

an interface to a recording medium;

an input port for receiving a video signal to be recorded on the medium;

a watermark detector coupled to the input port;

a data detector coupled to the input port to detect data at a predetermined location in the video signal; and

a processor coupled to compare the detected watermark to a compression function of the data, and to enable recording of the video signal onto the medium if the comparison is a match.

20. The video recorder of Claim 19, wherein the compression function is a hash function of a hash function of the data.

21. The video recorder of Claim 19, wherein the data is a cryptographic value.

22. A method of controlling playing of a video signal recorded on a medium, comprising the acts of:

playing the video signal from the media;

detecting a watermark in the video signal;

detecting data associated with the video signal;

subjecting the data to a compression function; and

allowing further playing of the video signal only if the watermark matches the compression function of the data.

23. The method of Claim 22, further comprising the act of applying an analog copy protection signal to the played video.

24. The method of Claim 22, wherein the compression function is a hash function.

25. The method of Claim 22, wherein the data is a cryptographic value.

26. A video player comprising:

an interface to a recording medium which outputs a video signal;

a watermark detector coupled to receive the video signal;

a data detector coupled to detect a data associated with the video signal;

a processor coupled to the watermark detector and data detector and which subjects the detected data to a compression function and compares the watermark to the compressed function of the data and allows further playing only if the comparison is a match.

27. The video player of Claim 26, wherein the compression function is a hash function of a hash function.

28. The video player of Claim 26, wherein the data is a cryptographic value.

29. A method of controlling copying of a video or audio signal, comprising the acts of:

supplying the audio or video signal;

embedding a first watermark in the audio or video signal;

transmitting the video or audio signal to a user; and

embedding a second watermark in the video or audio signal in response to an action by the user.

30. The method of Claim 29, where the action by the user is an indication relating to payment.

31. A method of controlling copying of a video or audio signal having an embedded watermark, comprising the acts of:

determining if recording of the video or audio signal is to be prevented;

if recording is to be prevented, adding a second watermark; and

transmitting the video or audio signal with the first and second watermarks.

32. The method of Claim 31, further comprising the acts of:

deciding if the recording is not to be prevented;

reporting that recording is not to be prevented; and

charging a fee for not preventing the recording.

33. The method of Claim 31, further comprising the acts of:

if recording is permitted, recording the audio or video signal; and

adding to the recorded audio or video signal the second watermark.

34. A set top video or audio box for connection to an associated receiver, comprising:

an input terminal adapted to receive a video or audio signal;

a conditional access control having a control terminal for receiving a selection enabling recording of the video or audio signal;

a watermark embedder for embedding a second watermark and having a control terminal coupled to an output terminal of the conditional access control and receiving the video or audio signal from the input terminal, and having an output terminal, wherein the video or audio signal

includes a first watermark; wherein the watermark embedder outputs the video or audio signal with the first and second watermarks in response to the conditional access control.

35. The set top box of Claim 34, further comprising:

a connection to an uplink or computer network, wherein the conditional access control transmits on the uplink/network an indication of the selection.

36. A method of operating a video or audio recorder, comprising the acts of:

receiving an input audio or video signal having a first and a second watermark;

detecting the watermarks;

preventing recording of the input video or audio signal if both the first and second watermarks are detected.

37. A video or audio recorder, comprising:

an interface to recording medium;

an input port for receiving a video or audio signal to be recorded;

a watermark detector coupled to the input port; and

a processor coupled to receive an indication of detected watermarks, and to prevent recording of the video or audio signal onto the media if two predetermined watermarks are detected.

38. The video or audio recorder of Claim 37, further comprising a watermark embedder operatively coupled to the processor.

39. A method of controlling playing of a video or audio signal recorded on a medium, comprising the acts of:

playing the video or audio signal from the medium;

detecting any watermarks in the video or audio signal; and

preventing further playing of the video or audio signal if detected watermarks match respectively two predetermined watermarks.

49. The method of Claim 39, further comprising the act of applying an analog copy protection signal to the played video or audio signal.

METHOD AND APPARATUS FOR ENHANCED AUDIO/VIDEO SERVICES WITH WATERMARKS AND ASSOCIATED DATA

Mark Alan Hollar
Peter Wonfor

Abstract

Method and apparatus for controlled copying of an audio or video signal transmitted over a cable television or direct satellite broadcast system or the internet. Copyrighted (or other) audio or video material is protected from unwanted copying (recording) by the combination of a watermark embedded in the audio or video signal at the head end together with additional copy protection data inserted in the audio or video signal, either a ticket or a second watermark. Video line 21 in the vertical blanking interval for (NTSC TV) is used to hold the ticket (cryptographic counter). An audio or video watermark is embedded in the active portion of the audio or video signal. Only if the consumer is willing to pay a fee is the video signal with both the watermark and the ticket transmitted to his recording device which then matches the watermark to a mathematical function of the ticket, and only if they match is recording permitted. Alternatively, this consumer control may operate on a second watermark in the audio or video. The corresponding playback device outputs an audio or video signal which does not have the ticket and hence no further copying is permitted. This enables a single copy to be made upon payment.

Figure 1A

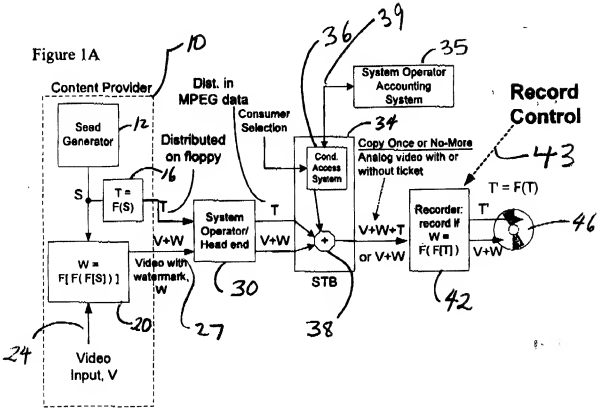
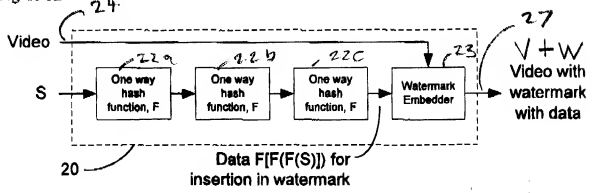


Figure 1B



6,987,720 - 12/26/2006

Figure 1C

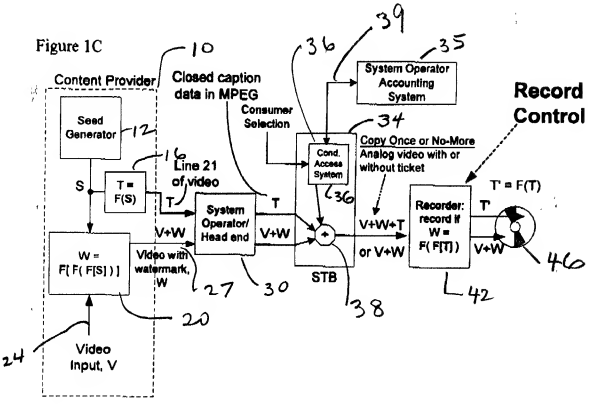


Figure 1D

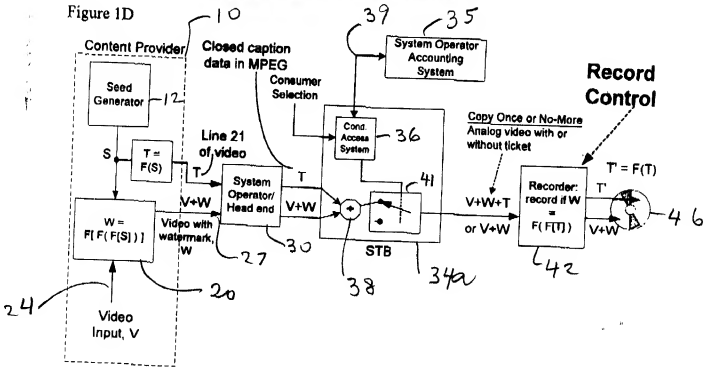


Figure 2

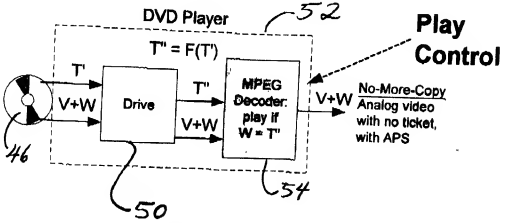


Figure 3

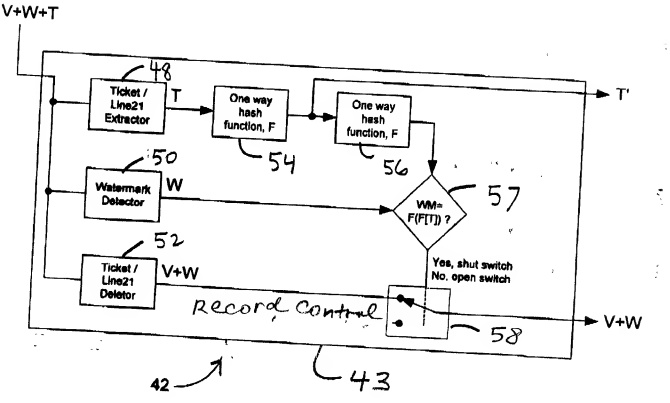

V+W+T
48
Ticket / Line21 Extractor
T
One way hash function, F
One way hash function, F
T'
54
56
50
Watermark Detector
W
57
WM= F(F[T]) ?
52
Ticket / Line21 Deletor
V+W
Yes, shut switch
No, open switch
Record control
V+W
58
42
43

Figure 4

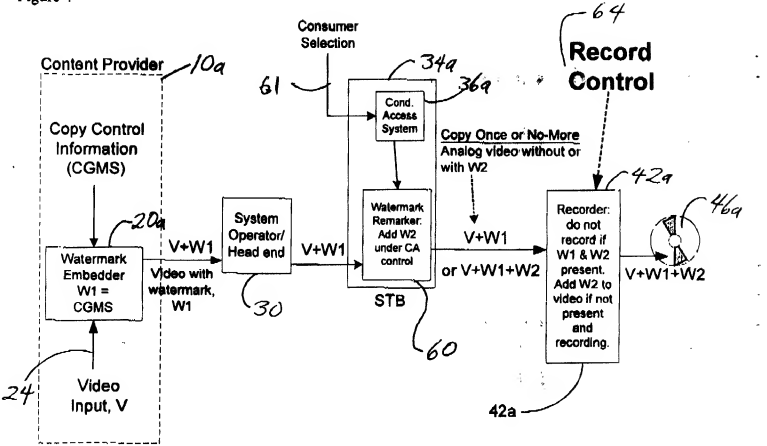
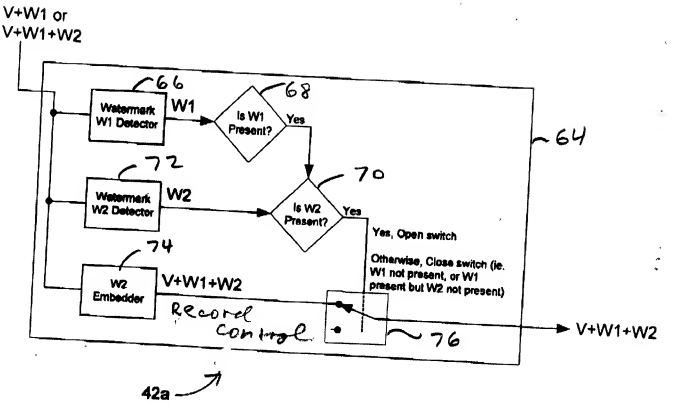

Content Provider
10a
Copy Control Information (CGMS)
20a
Watermark Embedder W1 = CGMS
24
Video Input, V
V+W1
Video with watermark, W1
System Operator/ Head end
30
V+W1
Consumer Selection
61
34a
36a
Cond. Access System
Watermark Remarker: Add W2 under CA control
STB
60
Copy Once or No-More
Analog video without or with W2
V+W1
or V+W1+W2
64
Record Control
42a
Recorder: do not record if W1 & W2 present. Add W2 to video if not present and recording.
46a
V+W1+W2
42a

Figure 5


V+W1 or
V+W1+W2
66
Watermark
W1 Detector
W1
68
Is W1
Present?
Yes
64
72
Watermark
W2 Detector
W2
70
Is W2
Present?
Yes
Yes, Open switch
Otherwise, Close switch (ie.
W1 not present, or W1
present but W2 not present)
74
W2
Embedder
V+W1+W2
Record
control
76
V+W1+W2
42a

Omotan 1265060

Figure 6A

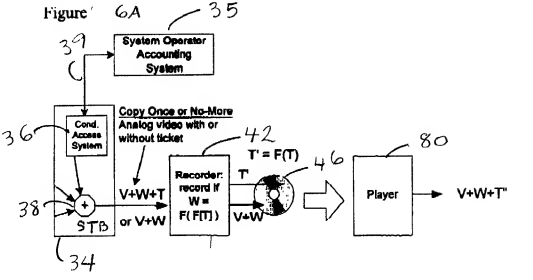


Figure 6B

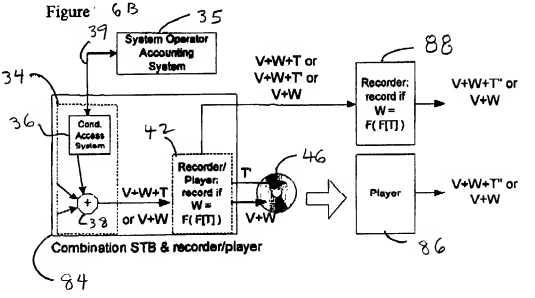


Figure 7

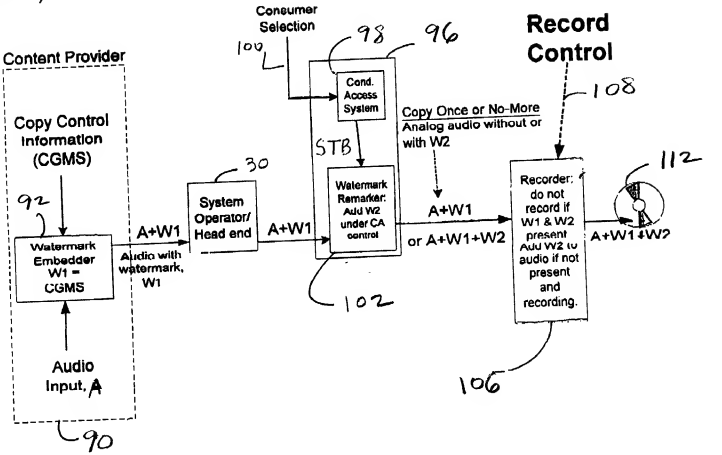
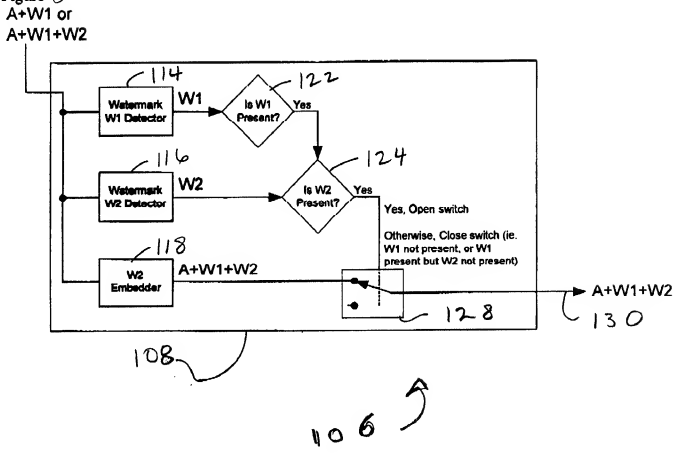

Content Provider
Copy Control Information (CGMS)
92
Watermark Embedder W1 = CGMS
Audio Input, A
90
A+W1
Audio with watermark, W1
30
System Operator/ Head end
A+W1
Consumer Selection
100
98
96
Cond. Access System
STB
Watermark Remarker: Add W2 under CA control
102
Copy Once or No-More
Analog audio without or with W2
A+W1
or A+W1+W2
Record Control
108
Recorder: do not record if W1 & W2 present Add W2 to audio if not present and recording.
106
112
A+W1+W2

Figure 8


A+W1 or
A+W1+W2
114
Watermark
W1 Detector
W1
122
Is W1
Present?
Yes
116
Watermark
W2 Detector
W2
124
Is W2
Present?
Yes
Yes, Open switch
Otherwise, Close switch (ie.
W1 not present, or W1
present but W2 not present)
118
W2
Embedder
A+W1+W2
A+W1+W2
128
130
108
106

DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below adjacent to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of subject matter (process, machine, manufacture, or composition of matter, or an improvement thereof) which is claimed and for which a patent is sought by way of the application entitled

Method And Apparatus For Enhanced Audio/Video Services With Watermarks And Associated Data

which (check) ☒ is attached hereto.
☐ and is amended by the Preliminary Amendment attached hereto.
☐ was filed on _____ as Application Serial No.
☐ and was amended on ___ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
Number	Country	Day/Month/Year Filed	Yes	No
N/A			☐	☐

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

Provisional Application Number	Filing Date
60/121,806	02/25/99

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) or PCT international application(s) designating the United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information, which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status (patented, pending, abandoned)
N/A		

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith:

Alan H. MacPherson (24,423); Brian D. Ogonowsky (31,988); David W. Heid (25,875); Norman R. Klivans (33,003); Edward C. Kwok (33,938); David E. Steuber (25,557); Michael Shenker (34,250); Stephen A. Terrile (32,946); Peter H. Kang (40,350); Ronald J. Meetin (29,089); Ken John Koestner (33,004); Omkar K. Suryadevara (36,320); David T. Millers (37,396); Kent B. Chambers (38,839); Michael P. Adams (34,763); Robert B. Morrill (43,817); Michael J. Halbert (40,633); Gary J. Edwards (41,008); James E. Parsons (34,691); Daniel P. Stewart (41,332); Philip W. Woo (39,880); John T. Winburn (26,822); Tom Chen (42,406); Fabio E. Marino (43,339); William W. Holloway (26,182); Don C. Lawrence (31,975); Marc R. Ascolese (42,268); Carmen C. Cook (42,433); David G. Dolezal (41,711); Roberta P. Saxon (43,087); Mary Jo Bertani (42,321); Dale R. Cook (42,434); Sam G. Campbell (42,381); Matthew J. Brigham (44,047); Hugh H. Matsubayashi (43,779); Patrick D. Benedicto (40,909); T.J. Singh (39,535); Shireen Irani Bacon (40,494); Rory G. Bens (44,028); George Wolken, Jr. (30,441); John A. Odozynski (28,769); Cameron K. Kerrigan (44,826); Kenneth C. Brooks (38,393); Paul E. Lewkowicz (44,870); Theodore P. Lopez (44,881); and Mayankkumar M. Dixit (44,064).

Please address all correspondence and telephone calls to:

Norman R. Klivans
Attorney for Applicant(s)
SKJERVEN, MORRILL, MacPHERSON, FRANKLIN & FRIEL LLP
25 Metro Drive, Suite 700
San Jose, California 95110-1349

Telephone: 408-453-9200
Facsimile: 408-453-7979

I declare that all statements made herein of my own knowledge are true, all statements made herein on information and belief are believed to be true, and all statements made herein are made with the knowledge that whoever, in any matter within the jurisdiction of the Patent and Trademark Office, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be subject to the penalties including fine or imprisonment or both as set forth under 18 U.S.C. 1001, and that violations of this paragraph may jeopardize the validity of the application or this document, or the validity or enforceability of any patent, trademark registration, or certificate resulting therefrom.

Full name of sole (or first joint) inventor: Mark A. Hollar

Inventor's Signature: _____ Date: _____

Residence: Palo Alto, California 94306

Post Office Address: 3395 Birch Street
Palo Alto, CA 94306

Citizenship: U.S.

Full name of second inventor: Peter Wonfor

Inventor's Signature: _____ Date: _____

Residence: El Granada, California 94018

Post Office Address: 962 Malaga
El Granada, CA 94018

Citizenship: U.S.